Release Notes: Version 07.6.04 Operating System

for the HP ProCurve Routing Switch 9304M, 9308M, and 9315M
with Redundant Management (M2, M4, EP, and T-Flow), Edition 2

Software release 07.6.04 supersedes earlier software releases in the 07.x software branch. (For more on software branches, see “Software Branches” on page 2.)

Minimum S/W Version:	Supported HP ProCurve Series 9300 Redundant Management Modules:
07.1.10 (9304M and 9308M Only)	• J4845A ProCurve 9300 GigLX Redundant Management Module (8-port, M2) • J4846A ProCurve 9300 GigSX Redundant Management Module (8-port, M2) • J4847A ProCurve 9300 Redundant Management Module (0-port, M2)
07.1.19 (9304M and 9308M Only)	• All of the redundant management modules listed for release 7.1.10. • J4857A HP ProCurve 9300 Mini-GBIC Redundant Management Module (8-port, M4)
07.5.04 (9304M, 9308M, and 9315M)	• All of the redundant management modules listed for release 7.1.19. • J4879A HP ProCurve 9300 T-Flow Redundant Management Module
07.6.00 (9304M, 9308M, and 9315M)	• All of the redundant management modules listed for release 7.5.04. • J4885A HP ProCurve 9300 EP Mini-GBIC Redundant Management Module

These release notes:

- Provide useful procedures, information, and notes for routing switch operation and management.
- Summarize the new operating system enhancements available in software release 07.6.04.
- Summarize earlier software operating problems fixed in software release 07.6.04.

Descriptions of the enhancements in release 07.6.04 are included in the manuals for the 07.6.04 release. If you purchased a Redundant Management module with software version 07.6.04 or greater installed, then the CD shipped with the module includes these manuals. Otherwise, you can download PDF versions of the latest manuals. (Refer to “Downloading the Latest Software and Documentation” on page 1.)

NOTES:

Software Update Notice: Check the HP ProCurve Website frequently for free software updates for various HP ProCurve switch products. (Refer to “Downloading the Latest Software and Documentation” on page 1.)

Mini-GBIC ports: Hewlett-Packard offers and supports only mini-GBICs having an HP label (with product number J4858A, J4859A, or J4860A) for use with the J4856A HP ProCurve 9300 Mini-GBIC Module and the J4857A HP ProCurve 9300 Mini-GBIC Redundant Management Module. Use of other brands of mini-GBICs is not supported.

Flash Images: The flash image files for this software release differ depending on the type of management module you use. Refer to “Software Image Files” on page 3.

SNMP: Beginning with software release 05.2.16, the software does not have a default read-write SNMP community. If you use the default community name “private” as the password for web management access or for read-write access through a network management application, you need to use the CLI to add the read-write community string first.

Devices Without Redundant Management: For information on upgrading the software on the 9304M and 9308M routing switches WITHOUT redundant management, refer to the latest 6.6.x release notes. (Refer to “Downloading the Latest Software and Documentation” on page 1.)

Publication Number

5990-6027
Edition 2
March 2004

Applicable HP ProCurve 9300 (Current) Products

9304M Routing Switch . . . . . (J4139A)
9308M Routing Switch . . . . . (J4138A)
9315M Routing Switch . . . . . (J4874A)

10/100 Module . . . . . (J4140A)
T-Flow RM Module . . . . . (J4879A)
EP 10/100-TX RJ-45 Module . . . . . (J4881A)
EP 10/100-TX Telco (RJ-21) Module . . . . . (J4889A)
EP Mini-GBIC RM Module . . . . . (J4885A)
1-Port 10 Gigabit Ethernet Module . . . . . (J4891A)
EP Mini-GBIC Module. . . . . (J4894A)
EP 100/1000-T Module. . . . . (J4895A)
2-Port 10 Gigabit Ethernet Module . . . . . (J8174A)
EP 100Base-FX Module . . . . . (J8178A)

Gigabit-SX-LC Mini-GBIC . . . . . (J4858A)
Gigabit-LX-LC Mini-GBIC . . . . . (J4859A)
Gigabit-LH-LC Mini-GBIC . . . . . (J4860A)

10 Gigabit Ethernet LR Optic . . . . . (J8173A)
10 Gigabit Ethernet SR Optic . . . . . (J8175A)
10 Gigabit Ethernet ER Optic . . . . . (J8176A)

Redundant Power Supply . . . . . (J4147A)
9315 Redundant Power Supply . . . . . (J4875A)

Trademark Credits

Microsoft®, Windows®, and Windows NT® are trademarks of Microsoft Corporation. Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. SuperSpan® is a trademark of Foundry Networks, Inc.

Disclaimer

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Blvd.
Roseville, CA 95747-5551
USA
http://www.hp.com/go/hpprocurve

Contents

Terminology

This table defines basic product terms used in HP ProCurve routing switch documentation.

Term	Definition
chassis *or* Chassis device	A routing switch that accepts optional modules or power supplies. The HP 9315M, HP 9304M, and HP 9308M routing switches are Chassis devices.
EP *and* Standard	Routing switches can be EP or Standard devices, depending on whether the management module is an EP or Standard (M2 or M4) module. For a listing of these devices with their product numbers, refer to “HP ProCurve Routing Switch 9300M Series Modules” on page 40.
routing switch *or* router	A Layer 3 device that switches and routes network traffic. The term *router* is sometimes used in this document in descriptions of a routing switch’s Layer 3 routing protocol features.
Switch	A Layer 2 device that switches network traffic.
`HP9308#`	An example Command Line Interface (CLI) prompt. Actual prompts show the product number for the device, such as `HP9308#`.

Downloading the Latest Software and Documentation

You can download software version 07.6.04 and the corresponding product documentation from HP’s ProCurve website as described below.

To Download a Software Version:

1. Go to HP’s ProCurve website at **http://www.hp.com/go/hpprocurve**
2. Click on **software** (in the sidebar).
3. Under “latest software”, click on **switches**.

Note: If you are downloading software for a 9304M or 9308M, select the option that matches the type of management module(s) you are using in the device (WITH redundant management or WITHOUT redundant management).

To Download Product Documentation:

NOTE: The documentation for release 07.6.04 is included on the Product Documentation CD-ROM shipped with management modules after October, 2003.

For the latest version of product documentation for the HP ProCurve routing switches:

1. Go to HP’s ProCurve website at **http://www.hp.com/go/hpprocurve**
2. Click on **technical support**, then **manuals**.
3. Click on the name of the product for which you want manuals.
4. On the page listing the manuals, find the latest manuals under the heading "**For software version 7.6.04 or greater**".

You will need the Adobe® Acrobat® Reader (version 4.0 or greater) to view and/or print the manuals.

Software Branches

Beginning with the software releases 06.6.28 and 07.1.10, HP offers three software (Operating System) branches:

Table 1. Software Branches

Software Version:	Typically Include:	Operate On:
06.6.28 and later 06.*x* releases	Bug Fixes	• HP 9304M and 9308M routing switches *without* redundant management (that is, with M1 modules) • HP 6308M-SX routing switch • HP 6208M-SX switch
07.1.10 and Greater 07.1.x Releases	New Features, Enhancements to Existing Features, and Bug Fixes	HP 9304M and 9308M routing switches WITH redundant management (M2 modules)
07.5.04 Release	New Features, Enhancements to Existing Features, and Bug Fixes	HP 9304M, 9308M, and 9315M routing switches WITH redundant management (M2 and M4 modules)
07.6.00 and 07.6.01b Releases	New Features, Enhancements to Existing Features, and Bug Fixes	HP 9304M, 9308M, and 9315M routing switches WITH redundant management (M2, M4, EP, T-Flow, and 1-port 10GB modules)
07.6.04 Release	New Features, Enhancements to Existing Features, and Bug Fixes	HP 9304M, 9308M, and 9315M routing switches WITH redundant management (M2, M4, EP, T-Flow, 1-port 10GB, and 2-port 10GB modules)

Already Using a 9304M or 9308M with Redundant Management? Here's New Information!

If you received a 9304M or 9308M before software release 07.6.04 began shipping, and you are updating the device to release 07.6.04, then you may want to examine the new product manuals that became available beginning with the 07.6.04 release. To view (and freely download) PDF versions of these manuals (whole manual, or chapter-by-chapter files). See "Downloading the Latest Software and Documentation" on page 1.

Also, if you are updating a redundant management module to software release 07.6.04 (or greater) from a 7.1.*x* (or earlier) release, you will need to boot the routing switch from a TFTP server to perform this task. Refer to "Updating Software (M2, M4, and EP) to Release 07.6.04" on page 6.

Software/Device Compatibility

Table 2. Device Compatibility with Software Versions

Devices	Software Versions:				
	04791 05084	H2R07504.BIN[1] H2R07600.BIN[2] H2R07601.BIN H2R07604.BIN	H2R05216.BIN H2R06605.BIN H2R06616.BIN H2R07110.BIN H2R07122.BIN H2R07124.BIN	HPR05216.BIN HPR06605.BIN HPR06616.BIN HPR06628.BIN HPR06633.BIN HPR06636.BIN	HPS05216.BIN HPS06605.BIN HPS06616.BIN HPS06628.BIN HPS06633.BIN HPS06636.BIN
HP ProCurve 9315M (J4174A) Routing Switch with EP or Standard Redundant Management Module(s)	*No*	**Yes**	*No*	*No*	*No*
HP ProCurve 9304M (J4139A) and 9308M (J4138A) Routing Switches *with EP or Standard Redundant Management Module(s)*	*No*	**Yes**	**Yes**	*No*	*No*
HP ProCurve Routing Switch 9304M (J4139A) and 9308M (J4138A) with an M1 Management Module (M1)	**Yes**	*No*	*No*	**Yes**	*No*
HP ProCurve Routing Switch 6308M-SX (J4840A)	*n/a*	*n/a*	*No*	**Yes**	*No*
HP ProCurve Switch 6208M-SX (J4841A)	*n/a*	*n/a*	*No*	*No*	**Yes**

[1] First software release to support the 9315M routing switch and the J4879A T-Flow module
[2] First software release to support the EP (Enhanced Performance) modules.

If you have a 9304M or 9308M routing switch that was shipped before the software versions described in this document were available, you can download this release from HP's ProCurve website. To do so, see the chapter titled "Using Redundant Management Modules" in the *Installation and Basic Configuration Guide* included on the CD-ROM shipped with your management module(s) and also available on the HP ProCurve website. (Refer to "Updating Software" on page 6.) Also, to update your routing switch software, refer to the chapter titled "Updating Software Images and Configuration Files" in the same *Installation and Basic Configuration Guide*.

Software Image Files

To run software release 07.6.04, you need the indicated boot and software images listed below.

NOTE: This software release operates only with Standard (M2 or M4), EP, and T-Flow Redundant Management modules. You cannot install and run this software on non-redundant (M1) management modules.

The 9315M Routing Switch requires a minimum of one Redundant Management Module running software release 07.5.04 or greater. This is true regardless of whether you plan to install a management module from a 9304M or 9308M that has been running an earlier release.

Due to the size of the 07.6.04 (or greater) OS software image, you cannot directly update the OS image in a Redundant Management Module if that module does not already have an 07.6.04 (or greater) image in flash memory. Thus to update a Redundant Management Module to release 07.6.04 (or greater) for the first time (for use in the 9304M, 9308M, or the 9315M with Redundant Management), you must first upgrade the routing switch *boot code* to 07.6.02 (or greater). To update an M2, M4, or EP management module from a software release earlier than 07.6.04, refer to "Updating Software" on page 6. To update a T-Flow management module from a release earlier than 07.6.04, refer to "Updating Software (T-Flow)" on page 8.

Release 07.6.04 includes Secure Shell (SSH) version 1.5 (HP 9304M, HP 9308M, and HP 9315M).

SSH is not available for the 9304M or 9308M with a 32MB management module ("Management 1" module). Also, Management 1 modules cannot be used with the 9315M.

Table 3. Software Image Requirements

Product	Modules	Boot Image	Software Image
HP 9304M HP 9308M	With one of these (discontinued) M1 modules; that is, WITHOUT Redundant Management: • J4141A 10/100 • J4144A Gigabit SX • J4146A Gigabit 4LX/4SX	M1B07108.bin or greater recommended	HPR06636.bin*
HP 9304M HP 9308M HP 9315M	With any one or two of these modules; that is, WITH Redundant Management: • J4846A Gigabit SX* (M2) • J4845A Gigabit LX* (M2) • J4847A 0-Port* (M2) • J4857A Mini-GBIC (M4) • J4885A EP • J4879A T-Flow	M2, M4, and EP: • M2B07602.bin or greater T-Flow Module: • M2B07.6.02 (all MP images) • VSB07100.bin (VSM code)	M2, M4, and EP: • H2R07604.bin T-Flow: • TSP07604.bin
	10-Gigabit Ethernet Modules **Note:** To update FPGA code, refer to "Updating an FPGA on a 10-Gigabit Ethernet Module" on page 11.	*The 10-Gigabit Ethernet modules do not use any of the above boot images.*	The Field-Programmable Gate Arrays (FPGAs) in these modules do not use any of the above software images. Instead, they use the following software. J4891A FPGA: • rxbmgr.bin – version 80, revision 6 • rxpp.bin – version 81, revision 16 • txaccum.bin – version 82, revision 6 • txpp.bin – version 83, revision 13 • ageram.bin – version 84, revision 4 J8174A FPGA: • xpp.bin – version 88, revision 37 • xtm.bin – version 89, revision 39 **Note**: To determine the versions that are running on the modules, enter **show flash**. The version information is listed separately for each 10-Gigabit Ethernet module in the chassis.

Product	Modules	Boot Image	Software Image
HP 6308M-SX		• M1B07108.bin or greater recommended	• HPR06636.bin*
HP 6208M-SX		• M1B07108.bin or greater recommended	• HPS06636.bin*

*Does not support Secure Shell (SSH) version 1.

NOTE: If you are adding a Gigabit Copper module to a 9304M or 9308M routing switch chassis, boot code version M2B07108.bin or later must be used in the routing switch.

If you are updating a routing switch image from software release 07.1.24 or earlier, you will not be able to load a higher software release into flash memory. Software release 07.1.24 and earlier support TFTP of files up to 2.8MB, but the 07.6.04 and greater images are larger.

Note Regarding New Features in the H2R Software

MRP and VSRP Included in Release 07.6.04 and Higher

Starting with release 07.6.04, the H2R routing switch image supports Metro Ring Protocol (MRP) and Virtual Switch Redundancy Protocol (VSRP).

SRP Removed

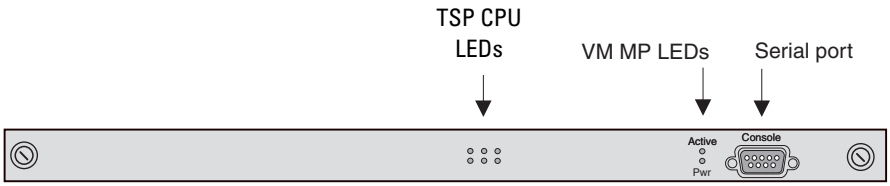
In software release 07.6.01 and greater, the HP Standby Router Protocol (SRP) has been removed.

Note to T-Flow Users

The LEDs for traffic received by TSP CPUs blink more frequently in software releases 07.5.04 and greater. This occurs because the module's processors exchange information more frequently in these releases than in earlier software releases, and this traffic is indicated by the LEDs. The increased blinking does not indicate an increase in data traffic received by the CPUs. The LEDs will blink even when there is no data traffic.

The LEDs for traffic received by the TSPs are the lower three LEDs in the group of six TSP CPU LEDs near the middle of the module.

Figure 1 T-Flow Module



To display TSP and VM CPU utilization information, enter the **show cpu** command.

Notes Regarding Monitoring of Router Traffic

- For inbound traffic that is routed (not switched), if the traffic is forwarded by the hardware and thus bypasses the CPU, the port that receives the traffic changes the source and destination MAC addresses of the packet before sending the packet to its outbound port and the mirror port.
- For outbound traffic that is routed (not switched), the source MAC address of the traffic that is copied to the mirror port has the MAC address of the mirror port rather than the monitored port's MAC address.

  This happens because the routed traffic sent by the router interface must address itself as the sender of the packet, to the neighboring router. This behavior cannot be turned off for the monitored traffic, so the mirror

port's MAC address is substituted for the mirror copy of the packet. In this case, the source MAC address of the mirror port is equivalent to that of the monitored port.

Updating Software

This section explains how to update software on the 9304M, 9308M, and 9315M, and contains these topics:

For easy software image management, all HP devices support the download and upload of software images between the flash modules on the devices and a Trivial File Transfer Protocol (TFTP) server on the network.

NOTE: HP recommends that you make a backup copy of the startup-config file before you update the software. If you need to run an older release, you will need to use the backup copy of the startup-config file.

The management module contains two flash memory modules:

- ***Primary flash*** – The default local storage area for image files and configuration files.
- ***Secondary flash*** – A second flash storage area. You can use the secondary flash to store redundant images for additional booting reliability or to preserve one software image while testing another one.

Only one flash area is active at a time. By default, the primary image will become active upon reload.

You can update the software contained in a flash area using TFTP to copy the update image from a TFTP server into the flash area. Also, you can copy software images and configuration files from a flash area to a TFTP server.

NOTE: HP devices are TFTP clients but not TFTP servers. You must perform the TFTP transaction from the HP device. You cannot "put" a file onto the HP device using the interface of your TFTP server.

Updating Software (M2, M4, and EP) to Release 07.6.04

Beginning with release 07.6.04, a new compression algorithm is used to generate software code images. The new compression algorithm allows the software images to contain more features. Boot code version 07.6.02 and later can decompress and load the new images. Boot code versions earlier than 07.6.02 cannot decompress and load the new images. Also, software code versions 07.6.01b and later can copy images that use the new compression method to flash memory. Earlier versions cannot.

(To determine which boot code version is running on your device, use the **show flash** command. The line that begins "Boot Image size" lists the boot code version, at the end of the line.)

This section explains how to load the boot code and software code on M2, M4, and EP management modules.

If you are updating redundant management modules, the software code is automatically copied from the active management module to the standby module when you reload. However, the boot code is not automatically copied. See the "Using Redundant Management Modules" chapter in the *Installation and Basic Configuration Guide*.

Updating the Boot Code (M2, M4, and EP)

NOTE: Software release 07.6.04 requires that you update the boot code on the management module to version 07.6.02. See "Updating Software (M2, M4, and EP) to Release 07.6.04" on page 6 for more information.

To update the boot code on a management module, use the following CLI method.

1. Place the new boot code on a TFTP server that the HP device can access.
2. Enter the following command at the Privileged EXEC level of the CLI (example: `HP9300#`) to copy the boot code from the TFTP server into the flash memory of the management module:

   copy tftp flash < *ip-addr* > < *image-file-name* > **boot**
3. Verify that the code has been successfully copied by entering the following command at any level of the CLI: **show flash**

   The line that begins "Boot Image size" lists the boot code version, at the end of the line.
   - If the boot code version is correct, go to Step 5.
   - If the boot code version is not correct, go to Step 2.
4. If the routing switch includes a redundant management module, synchronize the boot code on the redundant management module now by executing the **sync boot** command.
5. If the boot code version is correct, reload the software by entering one of the following commands:
   - **reload** (this command boots from the default boot source, which is the primary flash area by default)
   - **boot system flash primary | secondary**

Updating the Software Code (M2, M4, and EP)

NOTE: To update the software code, you first must update the boot code to 07.6.02 and boot the new software release from a TFTP server. After doing these steps, you can then use the **copy tftp flash** command to copy the new software code to flash memory.

To update to Release 07.6.04 from a Version *Earlier* than 07.6.01b:

1. Update the *boot code* on the management module and any redundant management modules to version 07.6.02. Refer to "Updating the Boot Code (M2, M4, and EP)", above.
2. Place the new software code (H2R07604.bin) on a TFTP server to which the HP device has access.
3. Execute the **reload** command.
4. Press **[B]** to stop the boot process and enter the boot monitor.
5. Enter an IP address.

   ip address < *ip-address* > < *subnet-mask* >
6. If the TFTP server is on a different subnet than the routing switch, enter the default gateway address the routing switch needs to reach the server.

   ip def < *default-gateway-address* >
7. Using the H2R07604.bin software you stored on the server in step 2, boot the routing switch from the TFTP server.

   boot system tftp < *server-ip-address* > h2r07604.bin
8. Update the software code on the primary management module to version 07.6.04.
9. *Wait for completion of the update:*
   - If there is not a redundant management module installed, you will see the message **TFTP to Flash Done** when the update is complete.
   - If there is a redundant management module installed, you will see the message **Sync secondary code in flash...Done** when the flash images are synchronized and the update is complete.

10. Verify that the software code has been successfully copied by entering the following command at any level of the CLI:

    show flash

    The line that begins “Compressed Pri Code size” lists the software code version in the primary flash, at the end of the line. Similarly, the line that begins “Compressed Sec Code size” lists the software code version in the secondary flash.

11. If the software code version is correct, go to Step 12. Otherwise, go to Step 2.
12. Execute the **reload** command.

NOTE: When you reload the software after updating the software code, the device displays a message stating that the configuration has changed and asking whether you want to save the changes. This occurs even if you do not make any configuration changes. The message occurs because the software code places its version number in the device's running-config when you load the code onto the device. You can select either to reload without saving the configuration change or save the change and reload. If the only change to the running-config is the software code version number, then your choice does not affect the operation of the device.

To update from release 07.6.01b to release 07.6.04:

1. If you have already updated the boot code on the management module to version 07.6.02, go to the next step. Otherwise, refer to “Updating the Boot Code (M2, M4, and EP)” on page 7.
2. Update the software code on the management module to version 07.6.04, then reload the software, below.

Updating Software (T-Flow)

This section explains how to load the boot or software code on the management processor (MP) or a T-Flow Switching Processor (TSP). The MP and TSPs run separate software. The MP runs chassis management software. The TSPs run Layer 2 and Layer 3 software. The procedures for updating MP and TSPs are different.

NOTE: The MP and TSP software code must have the same version number. Otherwise, the TSP functions are disabled. You can display the version numbers of the MP and TSPs by entering the **show vm-state** command. Also, if the version numbers are different, the command output displays a message.

HP recommends that you make a backup copy of the startup-config file before you update the software. If you need to run an older release, you will need to use the backup copy of the startup-config file.

If you are updating from a TFTP server, make sure the chassis has network (IP) access to the server.

When you reload the software after updating the software code, the device displays a message stating that the configuration has changed and asking whether you want to save the changes. This occurs even if you do not make any configuration changes. The message occurs because the software code places its version number in the device's running-config when you load the code onto the device. You can select either to reload without saving the configuration change or save the change and reload. If the only change to the running-config is the software code version number, then your choice does not affect the operation of the device.

Updating the Management Processor Boot Code

NOTE: Software release 07.6.04 requires that you update the MP boot code to version 07.6.02. See “Updating the Boot Code (M2, M4, and EP)” on page 7 for more information.

To update MP boot code from a TFTP server, enter a command such as the following:

```
HP9308# copy tftp flash 192.168.1.170 M2B07602.bin boot
```

Syntax: copy tftp flash < *ip-addr* > < *image-file-name* > boot

Updating the TSP Boot Code

NOTE: Software release 07.6.04 ***does not*** require that you update the TSP boot code, just the MP boot code.

To update TSP boot code from a TFTP server, enter a command such as the following:

```
HP9308# vm copy tftp flash 192.168.1.170 VSB07100.bin boot
```

Syntax: vm copy tftp flash < *ip-addr* > < *image-file-name* > boot

Updating the Management Processor Software Code

NOTE: If the device is running an MP software code version *earlier than* 07.6.01, refer to “To update to Release 07.6.04 from a Version Earlier than 07.6.01b:” on page 7 for more information.

To update MP software code (management software) from a TFTP server, enter a command such as the following:

```
HP9308# copy tftp flash 192.168.1.170 T1R07604.bin primary
```

This command copies Layer 3 software code from a TFTP server into the primary flash memory area for the MP. When you reload the software, the MP will boot the new code.

Syntax: copy tftp flash < *ip-addr* > < *image-file-name* > primary | secondary

To copy software code from one flash memory area to the other, enter a command such as the following:

```
HP9308# copy flash flash secondary
```

This command copies the software code in the primary flash memory area to the secondary flash memory area for the MP.

Syntax: copy flash flash primary | secondary

The **primary** parameter copies the image in the secondary flash area to the primary flash area.

The **secondary** parameter copies the image in the primary flash area to the secondary flash area.

Updating the TSP Software Code

To update the TSPs, enter a command such as the following at the Privileged EXEC level of the CLI:

```
HP9308# vm copy tftp flash 109.157.22.26 TSP07604.bin primary
```

This command updates the TSPs by copying a software code image from a TFTP server to the primary flash for each of the TSPs on the module.

To copy the software code from the primary flash to the secondary flash for each of the TSPs on the module, enter a command such as the following:

```
HP9308# vm copy flash flash secondary
```

Syntax: vm copy tftp flash < *tftp-server-ip-addr* > < *image-file-name* > primary | secondary

Syntax: vm copy flash flash primary | secondary

The **primary** and **secondary** parameters identify either the primary or secondary flash on the TSPs. For each command, the parameter specifies the destination of the copy operation.

Changing the Default Boot Source

By default, the T-Flow processors boot from the primary flash areas on the module. Each processor boots from its own primary flash. The MP boots first, then the TSPs boot.

You can change the default boot source to one of the following:

- Primary flash (the default)
- Secondary flash
- Interactive

The interactive option pauses during bootup of the TSPs to allow you to select the boot source for the TSPs. You must use this method if you want to boot the TSPs from a TFTP server. Otherwise, this method is used for troubleshooting.

To change the default boot source, enter commands such as the following at the global CONFIG level of the CLI:

```
HP9308(config)# vm boot secondary
HP9308(config)# write memory
```

This command configures the module to boot from the secondary flash by default.

NOTE: The **write memory** command saves the change to the startup-config file. You must save the configuration change for the change to remain in effect after you reboot.

Syntax: vm boot primary | secondary | interactive

The **primary** and **secondary** parameters specify a flash memory location. The **interactive** parameter causes the device to pause during bootup to allow you to specify the boot source for the TSPs. You must use this method if you want to boot the TSPs from a TFTP server. Otherwise, the **interactive** parameter is used for troubleshooting.

To configure the module to pause during booting to allow you to specify the boot source, enter the following command:

```
HP9308(config)# vm boot interactive
```

After you set the boot source to interactive and reboot, enter a command such as the following at the Privileged EXEC level of the CLI to boot the TSPs:

```
HP9308# vm boot tftp 192.168.1.170 vsb07100.bin
```

This command copies the TSP software code image from the specified TFTP server to a TSP address space from which the TSP can boot.

Syntax: vm boot primary | secondary | tftp < *ip-addr* > < *image-file-name* >

Updating an FPGA on a 10-Gigabit Ethernet Module

This section explains how to update an FPGA (Field-Programmable Gate Array) on single-port, 10-Gigabit Ethernet modules. These modules do not have boot code separate from the management module. However, they do have FPGAs that require separate software.

NOTE: The J8174A 2-port 10-Gigabit Ethernet module with XENPAK optics uses a different FPGA file than the older J4891A 1-port 10-Gigabit Ethernet module. See the table on page 4 for a list of the required FPGA files for both kinds of modules.

The J8174A 2-port 10-Gigabit Ethernet module with XENPAK optics can function in the same chassis with the older J4891A 1-port 10-Gigabit Ethernet module.

If an update is required for any of the FPGA files, you must update all the FPGA files.

1. Complete the updates of the boot code and software code, if required.
2. Enter commands such as the following (for the 1-port 10-Gig module) at the Privileged EXEC level of the CLI:

```
HP9308# 10gig copy tftp flash 10.10.10.10 rxbmgr.bin
HP9308# 10gig copy tftp flash 10.10.10.10 rxpp.bin
HP9308# 10gig copy tftp flash 10.10.10.10 txaccum.bin
HP9308# 10gig copy tftp flash 10.10.10.10 txpp.bin
HP9308# 10gig copy tftp flash 10.10.10.10 ageram.bin
```

   (The 2-port 10-Gig module has just two such files; xpp.bin and xtm.bin. Refer to ***"Software Image Requirements" on page 4***.)

   Syntax: 10gig copy tftp flash < *ip-addr* > < *filename* > [module < *slotnum* >]

   where:

   - **tftp** – specifies the location of the FPGA file. The **tftp** parameter shows that the file is on a TFTP server.
   - < *ip-addr* > – specifies the IP address of the TFTP server, if you specify **tftp**.
   - < *filename* > – specifies the FPGA file name.

   NOTE: You can store and copy the FPGA files using any valid filename. You are not required to store and copy the files using the names listed in "Software Image Files" on page 3. The device uses information within the files to install them in the correct FPGAs, and the **show flash** command lists the FPGAs according to the names in "Software Image Files" on page 3.

   - **module** < *slotnum* > – optionally, specifies the modules on which you want to install the update. If you do not specify a slot number, the command updates the FPGA on all 10-Gigabit Ethernet modules in the chassis.

3. Reload the software by entering one of the following commands:
   - **reload** (this command boots from the default boot source, which is the primary flash area by default)
   - **boot system flash primary | secondary**

   NOTE: The **show flash** command will list the new FPGA code versions but the new versions do not take effect until you reload the software.

Using SNMP to Update Software

You can use a third-party SNMP management application such as HP OpenView to update software on a routing switch.

NOTE: In software releases earlier than 07.5.04, the SNMP agent does not check for type validity with the SNMP version. In software release 07.5.04 and greater, the SNMP agent does not send a reply for a varbind, if the type of the varbind is not a known type for that version of SNMP. For example, MIB objects of type Counter64 cannot

be retrieved using a v1 packet, as Counter64 is a v2c and v3 type.

Make sure you use the correct procedure for your device and processor type. For example, do not use the Management Processor procedure to update the Switching Processors on a T-Flow module.

The syntax shown in this section assumes that you have installed HP OpenView in the "/usr" directory.

HP recommends that you make a backup copy of the startup-config file before you update the software. If you need to run an older release, you will need to use the backup copy of the startup-config file.

Using SNMP To Update a Chassis Module's Management Processor

Use this procedure to update the following:

- An M2, M4, or EP module
- The management processor on the T-Flow

To update software code on the Management Processor:

1. Configure a read-write community string on the HP device, if one is not already configured. To configure a read-write community string, enter the following command from the global CONFIG level of the CLI:

   snmp-server community < *string* > **ro | rw**

   where < *string* > is the community string and can be up to 32 characters long.

2. On the HP device, enter the following command from the global CONFIG level of the CLI:

   no snmp-server pw-check

   This command disables password checking for SNMP set requests. If a third-party SNMP management application does not add a password to the password field when it sends SNMP set requests to an HP device, by default the HP device rejects the request.

3. From the command prompt in the UNIX shell, enter the following command:

   /usr/OV/bin/snmpset -c < *rw-community-string* > < *hp-ip-addr* > **1.3.6.1.4.1.1991.1.1.2.1.5.0 ipaddress** < *tftp-ip-addr* > **1.3.6.1.4.1.1991.1.1.2.1.6.0 octetstringascii** < *file-name* > **1.3.6.1.4.1.1991.1.1.2.1.7.0 integer** < *command-integer* >

   where:

   < *rw-community-string* > is a read-write community string configured on the HP device.

   < *hp-ip-addr* > is the HP device's IP address.

   < *tftp-ip-addr* > is the TFTP server's IP address.

   < *file-name* > is the image file name.

   < *command-integer* > is one of the following:

   20 – Download the software code into the device's primary flash area.

   22 – Download the software code into the device's secondary flash area.

Using SNMP To Update Switching Processors on a T-Flow Module

This procedure updates the Switching Processors on the T-Flow module.

To update software code on the Switching Processors:

1. Configure a read-write community string on the HP device, if one is not already configured. To configure a read-write community string, enter the following command from the global CONFIG level of the CLI:

   snmp-server community < *string* > **ro | rw**

   where < *string* > is the community string and can be up to 32 characters long.

2. On the HP device, enter the following command from the global CONFIG level of the CLI:

   no snmp-server pw-check

   This command disables password checking for SNMP set requests. If a third-party SNMP management application does not add a password to the password field when it sends SNMP set requests to an HP device, by default the HP device rejects the request.

3. From the command prompt in the UNIX shell, enter the following command:

   /usr/OV/bin/snmpset -c < *rw-community-string* > < *hp-ip-addr* > **1.3.6.1.4.1.1991.1.1.2.1.5.0 ipaddress** < *tftp-ip-addr* > **1.3.6.1.4.1.1991.1.1.2.1.6.0 octetstringascii** < *file-name* > **1.3.6.1.4.1.1991.1.1.2.1.56.0 integer** < *module-type* > **1.3.6.1.4.1.1991.1.1.2.1.57.0 integer** < *slotnum* > **1.3.6.1.4.1.1991.1.1.2.1.7.0 integer** < *command-integer* >

   where:

   < *rw-community-string* > is a read-write community string configured on the HP device.

   < *hp-ip-addr* > is the HP device's IP address.

   < *tftp-ip-addr* > is the TFTP server's IP address.

   < *file-name* > is the image file name.

   < *module-type* > is the following:

   2 – T-Flow module.

   < *slotnum* > is the slot that contains the module you are updating. To update all modules of the type you specified, enter 0 (zero):

   < *command-integer* > is one of the following:

   24 – Download the software code into the device's primary flash area.

   25 – Download the software code into the device's secondary flash area.

General Note About Removing Chassis Modules

Before you remove a module from a chassis, disable the module. Disabling the module before removing it prevents a brief service interruption on other unmanaged modules. The brief interruption can be caused by the chassis re-initializing other modules in the chassis when you remove an enabled module.

NOTE: This section does not apply to the active or standby Redundant Management modules. The **disable module** and **enable module** commands are not applicable to management modules.

To disable a module, enter a command such as the following at the Privileged EXEC level of the CLI:

```
HP9308# disable module 3
```

This command disables the module in slot 3.

Syntax: disable module < *slot-num* >

The < *slot-num* > parameter specifies the slot number.

- Slots in a 4-slot chassis are numbered 1 – 4, from top to bottom.
- Slots in an 8-slot chassis are numbered 1 – 8, from left to right.
- Slots in a 15-slot chassis are numbered 1 – 15, from left to right.

NOTE: If you remove the module without first disabling it, the chassis re-initializes the other modules in the chassis, causing a brief interruption in service after which the chassis resumes normal operation.

You do not need to enable a module after inserting it in the chassis. The module is automatically enabled when you insert the module into a live chassis or when you power on the chassis.

If you plan to replace the removed module with a different type of module, you must configure the slot for the module. To configure a slot for a module, use the **module** command at the global CONFIG level of the CLI.

If, after disabling a module, you decide not to remove the module, re-enable the module using the following command:

Syntax: enable module < *slot-num* >

For example, to re-enable a module in slot 3:

```
HP9308# enable module 3
```

Note on Inserting or Removing an EP Module

NOTE: This section applies only to a 15-slot chassis containing EP modules.

Do not insert or remove EP modules in a 15-slot chassis until the chassis has fully booted. Generally, booting takes around two minutes. You can determine whether the device has fully booted by looking at the management console. Once the device boots, a command prompt or login prompt is displayed.

Once the device has booted, allow the device to fully complete the removal or insertion before removing or inserting another module. Generally, this takes about 30 seconds. After you remove or insert a module, the CLI displays a message confirming completion of the change. Wait for this message before removing or inserting another module.

Redundant Management on the 9304M, 9308M, and 9315M Routing Switches

Redundant Management means that the device can operate with two management modules installed; one active (primary) and one standby (secondary). If the active management module becomes unavailable, the standby management module automatically takes over system operation.

Management modules WITH Redundant Management capabilities are termed “M2”, “M4”, EP, or T-Flow modules. These modules include:

- J4857A HP ProCurve 9300 Mini-GBIC Redundant Management Module (8-port, M4)
- J4885A HP ProCurve 9300 EP Mini-GBIC Redundant Management Module (8-port)
- J4879A HP ProCurve 9300 T-Flow Redundant Management Module (0-port)
- J4845A ProCurve 9300 GigLX Redundant Management Module (8-port, M2 — *discontinued*)
- J4846A ProCurve 9300 GigSX Redundant Management Module (8-port, M2 — *discontinued*)
- J4847A ProCurve 9300 Redundant Management Module (0-port, M2 — *discontinued*)

If you are using a Redundant Management module, you can install either one or two such modules in the routing switch, as shown Table 4.

Table 4. Supported Management Module Combinations

Primary Management Module Type	Secondary (Redundant) Management Module Type	Notes
Any M2 or M4 Redundant Management Module	Another M2 or M4 Redundant Management Modules	Where an M2 and an M4 are used in the same switch, HP recommends using the faster M4 as the primary redundant management module. If the M4 fails, the system will use the slower M2 module.
J4885A EP Mini-GBIC Redundant Management Module	Another EP Redundant Management Module	
J4879A T-Flow Redundant Management Module	Another J4879A T-Flow Redundant Management Module	
Any M1 Management Module (*Discontinued*)	*n/a*	Supported only in the 9304M and 9308M routing switches. No redundant management options.

NOTE: M1 management modules, M2/M4 redundant management modules, EP redundant management modules, and T-Flow redundant management modules are *mutually exclusive*. That is, a routing switch does not operate if two redundant management modules of different types are installed. Also, M1 management modules do not operate in a 9315M routing switch.

For more information, see the chapter titled “Using Redundant Management Modules” in the *Installation and Basic Configuration Guide* that is included on the *Documentation CD-ROM* shipped with your management module, and also downloadable from the HP ProCurve website. (Refer to “To Download Product Documentation:” on page 1.)

These notes also contain information regarding what happens when you disable BGP4, OSPF, or VRRP. See “Usage Guidelines for Access Control Lists (ACLs)” on page 18.

Non-Redundant Management on the 9304M and 9308M Routing Switches

Management modules WITHOUT Redundant Management are sometimes termed “M1” modules (for “Management 1”). These modules, now discontinued, operate only in the 9304M and 9308M routing switches. M1 modules include:

- J4141A HP ProCurve 9300 10/100 Management Module (16-port)
- J4144A HP ProCurve 9300 Gigabit SX Management Module (8-port)
- J4146A HP ProCurve 9300 Gigabit 4LX/4SX Management Module (8-port)
- J4840A HP ProCurve 6308M-SX Routing Switch

NOTE: *M1 management modules do not operate in the 9315M routing switch.*

Also, if you are using an M1 management module in a 9304M or 9308M, no other management module (non-redundant or redundant) can be installed in the routing switch.

Maximum File Sizes for Startup-Config and Running-Config Files

Each HP device has a maximum allowable size for the running-config and the startup-config file. If you use TFTP to load additional information into a device's running-config or startup-config file, it is possible to exceed the maximum allowable size. If this occurs, you will not be able to save the configuration changes.

The following table lists the maximum size for the running-config and the startup-config file on HP devices.

Product type	Maximum running-config and startup-config file sizes[a]
A 9315 using Management II or higher	256K
A 9304M or 9308M using Management II or higher	256K
A 9304M or 9308M using Management I	128K
A 6308M-SX or 6208M-SX	64K

a.The running-config and startup-config file can each be the size listed. The maximum size is not the maximum combined size for the running-config and startup-config files.

To determine the size of an HP device's running-config or startup-config file, copy it to a TFTP server, then use the directory services on the server to list the size of the copied file. To copy the running-config or startup-config file to a TFTP server, use one of the following commands.

- Command to copy the running-config to a TFTP server:

  copy running-config tftp < *ip-addr* > < *filename* >

- Command to copy the startup-config file to a TFTP server:

  copy startup-config tftp < *ip-addr* > < *filename* >

Configuration Considerations for the 15-Slot Chassis (9315M)

Use the following considerations when configuring your 15-slot Chassis device.

Updating from Earlier Software

The 15-slot chassis requires software release 07.5.04 or greater. This is true regardless of whether you plan to install a management module from a 4-slot or 8-slot chassis that has been running an earlier software release.

To update a management module from a release earlier than 07.5.04, refer to "Updating Software (M2, M4, and EP) to Release 07.6.04" on page 6.)

Removing a Module from an Active Chassis

To remove a module from a chassis, disable the module first before removing the module from the chassis. Refer to "General Note About Removing Chassis Modules" on page 13.

NOTE: If you remove a module without first disabling it, the chassis re-initializes other modules in the chassis, causing a brief interruption in service after which the chassis resumes normal operation.

Slot Locations for Redundant Management Modules

The 15 slots in the chassis are divided among 4 internal regions. Slots 1 – 4 belong to the same region; slots 5 – 8 belong to the same region; slots 9 – 12 belong to the same region, and slots 13 – 15 belong to the same region. If you are using redundant management modules, HP recommends that you place both management modules in slots belonging to the same region. For example, if you place one management module in slot 5, HP recommends that you place the other management module in slot 6, 7, or 8.

MAC Addresses

The 15-slot chassis makes use of locally administered MAC addresses. If your site already uses locally administered MAC addresses of the vendor OUI, which is 00e052, there could be a MAC address conflict with one of the ports on the HP device.

Server Trunk Groups

If you plan to configure ports on a module into a server trunk group, use the following guideline:

- For a multi-slot trunk group (one configured on two forwarding modules), the modules must both be in the same set of slots (slots 1 – 7 or 9 – 15).

You do not need to follow this guideline for a switch trunk group.

NOTE: In software releases prior to 07.6.00, the management module(s) and the module that had the server trunk group's ports were required to be in the same set of slots (slots 1 – 7 or 9 – 15). In software release 07.6.00 and later, there is no longer a restriction on the location of the management module relative to the module used for server trunking. However, it is still a requirement that the module that has the server trunk group's lead ports cannot reside in slot 8.

VLANs

In release 07.6.01b, you could configure only up to 2195 Layer 2 VLANs on a 15-slot Chassis device. The **system-max vlan < *num* >** command allowed you to allocate a higher number of VLANs, but the software allowed you to actually create only 2195 of the allocated VLANs.

Starting In release 07.6.04, this restriction has been removed. You can create the full number of allocated Layer 2 VLANs on a 15-slot Chassis device, up to 4095.

Change to the Maximum Number of VLANs and Virtual Interfaces on M2, M4, EP, and T-Flow Devices

Table 5 lists the default and configurable maximum numbers of VLANs and virtual interfaces for routing switches in software release 07.5.04 and later. Unless otherwise noted, the values apply to both types of switches.

Table 5. VLAN and Virtual Interface Support

Product	VLANs		Virtual Interfaces	
	Default Maximum	Configurable Maximum	Default Maximum	Configurable Maximum
EP AND T-FLOW with 512MB	32	4095	255	4095
M4 management module with 256MB	32	4095	255	4095
M2 management module with 128MB management module	16	4095	255	512
M1 with 32MB	16	256	64	255

Usage Guidelines for Access Control Lists (ACLs)

This section provides some guidelines for implementing ACLs to ensure wire-speed ACL performance.

For optimal ACL performance, use the following guidelines:

- Apply ACLs to inbound traffic rather than outbound traffic.
- Use the default filtering behavior as much as possible. For example, if you are concerned with filtering only a few specific addresses, create deny entries for those addresses, then create a single entry to permit all other traffic. For tighter control, create explicit permit entries and use the default deny action for all other addresses.
- Use deny ACLs sparingly. When a deny ACL is applied to an interface, the software sends all packets sent or received on the interface (depending on the traffic direction of the ACL) to the CPU for examination.
- Adjust system resources if needed:
  - If IP traffic is going to be high, increase the size of the IP forwarding cache to allow more routes. To do so, use the **system-max ip-cache < num >** command at the global CONFIG level of the CLI.
  - If much of the IP traffic you are filtering is UDP traffic, increase the size of the session table to allow more ACL sessions. To do so, use the **system-max session-limit < num >** command at the global CONFIG level of the CLI.

Avoid the following implementations when possible:

- Do not apply ACLs to outbound traffic. The system creates separate inbound ACLs to ensure that an outbound ACL is honored for traffic that normally would be forwarded to other ports.
- Do not enable the strict TCP ACL mode unless you need it for tighter security.
- Avoid ICMP-based ACLs where possible. If you are interested in providing protection against ICMP Denial of Service (DoS) attacks, use HP's DoS protection features. See the chapter titled "Protecting Against Denial of Service Attacks"in the *Advanced Configuration and Management Guide* included on the Documentation CD-ROM shipped with your management module(s). Also, the latest version of this guide is available on the HP ProCurve website. (Refer to "Updating Software" on page 6.)

If the IP traffic in your network is characterized by a high volume of short sessions, this also can affect ACL performance, since this traffic initially must go to the CPU. All ICMP ACLs go to the CPU, as do all TCP SYN, SYN/ACK, FIN, and RST packets and the first UDP packet of a session.

ACL Support on the HP Products

HP ACLs have two basic types of uses:

- Filtering forwarded traffic through the device
- Controlling management access to the device itself

In general, routing switches support both types of ACLs. However, the 6208M-SX switch supports ACLs only for access control.

The following table lists the ACL functions supported on each HP routing switch supported in this software release.

Product	Packet Forwarding ACLs Supported	Management Access ACLs Supported
9304M, 9308M, and 9315M	Yes	Yes
6308M-SX	Yes	Yes
6208M-SX	No	Yes

Using ACLs and Network Address Translation (NAT) on the Same Interface

You can use ACLs and NAT on the same interface, so long as you follow these guidelines:

- Do not enable NAT on an interface until you have applied ACLs (as described below) to the interface. If NAT is already enabled, you must disable it, apply the ACLs, then re-enable NAT on the interface.
- Enable the strict TCP mode.
- On the inside NAT interface (the one connected to the private addresses), apply inbound ACLs that permit TCP, UDP, and ICMP traffic to enter the device from the private sub-net.

You can use a standard ACL to permit all traffic (including TCP, UDP, and ICMP traffic) or an extended ACL with separate entries to explicitly permit TCP, UDP, and ICMP traffic.

NOTE: You do not need to apply ACLs to permit TCP, UDP, and ICMP traffic unless you are applying other ACLs to the interface as well. If you do not plan to apply any ACLs to a NAT interface, then you do not need to apply the ACLs to permit TCP, UDP, and ICMP traffic.

Here is an example of how to configure a device to use ACLs and NAT on the same interfaces. In this example, the inside NAT interface is port 1/1 and the outside NAT interface is port 2/2.

The following commands enable the strict TCP mode and configure an ACL to permit all traffic from the 10.10.200.x sub-net. A second ACL denies traffic from a specific host on the Internet.

```
HP9308(config)# ip strict-acl-tcp
HP9308(config)# access-list 1 permit 10.10.200.0 0.0.0.255
HP9308(config)# access-list 2 deny 209.157.2.184
```

The following commands configure global NAT parameters.

```
HP9308(config)# ip nat inside source list 1 pool outadds overload
HP9308(config)# ip nat pool outadds 204.168.2.1 204.168.2.254 netmask 255.255.255.0
```

The following commands configure the inside and outside NAT interfaces. Notice that the ACLs are applied to the inbound direction on the inside NAT interface, and are applied *before* NAT is enabled. In this example, ACL 1 permits all traffic to come into the inside interface from the private sub-net. ACL 2 denies traffic from a specific host from going out the interface to the private sub-net.

```
HP9308(config)# interface ethernet 1/1
HP9308(config-if-e1000-1/1)# ip address 10.10.200.1 255.255.255.0
HP9308(config-if-e1000-1/1)# ip access-group 1 in
HP9308(config-if-e1000-1/1)# ip access-group 2 out
HP9308(config-if-e1000-1/1)# ip nat inside
HP9308(config-if-e1000-1/1)# interface ethernet 2/2
HP9308(config-if-e1000-2/2)# ip address 204.168.2.78 255.255.255.0
HP9308(config-if-e1000-2/2)# ip nat outside
```

Where to Find More Information

- For traffic filtering ACLs, refer to the chapter titled “IP Access Control Lists (ACLs)“in the *Advanced Configuration and Management Guide*.
- For management access ACLs, refer to the chapter titled “Securing Access to Management Functions“in the *Security Guide*.
- For DoS protection features, refer to the chapter titled “Protecting Against Denial of Service Attacks“in the *Advanced Configuration and Management Guide*.
- For information about IP access policies, see the “IP Access Policies“section in the “Policies and Filters” appendix in the *Advanced Configuration and Management Guide*.
- For NAT configuration information, see the “Network Address Translation“chapter in the *Advanced Configuration and Management Guide*.

Where To Find Documentation: All of the above manuals are included on the *Documentation CD-ROM* shipped with your management module(s). Also, the latest version of these guides are available on the HP ProCurve website. (Refer to “Updating Software” on page 6.)

Note Regarding Disabling BGP4, OSPF, or VRRP

You can easily disable a routing protocol using the CLI or Web management interface. However, be careful when you disable BGP4, OSPF, or VRRP. When you disable these protocols, the routing switch removes all the configuration information for the disabled protocol from the running-config. Moreover, when you save the configuration to the startup-config file after disabling one of these protocols, all the configuration information for the disabled protocol is removed from the startup-config file.

The CLI displays a warning message such as the following:

```
HP9300(config-bgp-router)# no router bgp
router bgp mode now disabled. All bgp config data will be lost when writing to
flash!
```

The Web management interface does not display a warning message.

If you have disabled the protocol but have not yet saved the configuration to the startup-config file, you can restore the configuration information by re-entering the command to enable the protocol (ex: **router bgp**), or by selecting the web management option to enable the protocol. If you have already saved the configuration to the startup-config file, the information is gone.

If you are testing a BGP4, OSPF, or VRRP configuration and are likely to disable and re-enable the protocol, you might want to make a backup copy of the startup-config file containing the protocol’s configuration information. This way, if you remove the configuration information by saving the configuration after disabling the protocol, you can restore the configuration by copying the backup copy of the startup-config file onto the flash memory.

Note to IP Multicast Users

HP routing switches support the following IP multicast versions:

- IGMP V2
- PIM Dense mode (PIM-DM) V1
- PIM Sparse mode (PIM-SM) V2
- DVMRP V2

For configuration information, see the “Configuring IP Multicast Protocols” chapter in the *Advanced Configuration and Management Guide provided for software release 07.5.x (or greater)*.

Clarification On Trunk Load Sharing

HP devices load share traffic across the ports in a trunk group. The method used for the load sharing depends on the following:

- Device type – 9304M/9308M/9315M (chassis) or 6308M-SX and 6208M-SX (fixed-port)
- Traffic type – Layer 2 or Layer 3
- Trunk type – Switch or server
- For certain traffic, port type on which the traffic enters the HP device (Gigabit or 10/100)

NOTE: The port type applies only to Layer 2 traffic on a server trunk group.

Table 6 lists how HP devices load share traffic across the ports in a trunk group on a 9304M, 9308M, or 9315M.

Table 6. HP Trunk Group Load Sharing – 9304M/9308M/9315M

Traffic Layer	Trunk Group Type	Traffic Type	Load-Sharing Basis
Layer 2	Switch	All traffic types	Destination MAC address
	Server	IP received on 10/100 port	Hash value derived from source and destination IP addresses
		IPX received on 10/100 port	Hash value derived from source and destination IPX addresses
		AppleTalk received on 10/100 port	Hash value derived from source and destination AppleTalk addresses
		Other traffic types received on 10/100 port	Hash value derived from source and destination MAC address
		All traffic types received on Gigabit port	Gigabit Port number on which traffic was received
Layer 3	Switch	IP	Destination IP address
		IPX	Destination IPX address
		AppleTalk	Destination AppleTalk address
		All other traffic types	Destination MAC address
	Server	IP	Destination IP address
		IPX	Destination IPX address
		AppleTalk	Destination AppleTalk address
		All other traffic types	Destination MAC address

Table 7 lists how HP devices load share traffic across the ports in a trunk group on a 6308M-SX or 6208M-SX.

NOTE: The 6308M-SX and 6208M-SX use the 06.*x* software branch (page 2) and are no longer offered by Hewlett-Packard.

Table 7. HP Trunk Group Load Sharing – 6308M-SX or 6208M-SX

Traffic Layer	Trunk Group Type	Traffic Type	Load-Sharing Basis
Layer 2	Switch	All traffic types	Destination MAC address
	Server	IP	Hash value derived from source and destination IP addresses
		IPX	Hash value derived from source and destination IPX addresses
		AppleTalk	Hash value derived from source and destination AppleTalk addresses
		Other traffic types	Hash value derived from source and destination MAC address
Layer 3	Switch	IP	Source and destination IP addresses
		IPX	Source and destination IPX addresses
		AppleTalk	Source and destination AppleTalk addresses
		Other traffic types	Source and destination MAC address
	Server	IP	Source and destination IP addresses
		IPX	Source and destination IPX addresses
		AppleTalk	Source and destination AppleTalk addresses
		All other	Source and destination MAC address

Recovering from a Lost Password

By default, the CLI does not require passwords. However, if someone has configured a password for the HP device but the password has been lost, you can regain super-user access to the device using the following procedure.

NOTE: Recovery from a lost password requires direct access to the serial port and a system reset.

To recover from a lost password:

1. Start a CLI session over the serial interface to the device.
2. Reboot the device.
3. While the system is booting, before the initial system prompt appears, enter **b** to enter the boot monitor mode.
4. Enter **no password** at the prompt. (You cannot abbreviate this command.) This command causes the device to bypass the system password check.
5. Enter **boot system flash primary** at the prompt.
6. After the console prompt reappears, assign a new password.

Corrections to the Manuals for Release 07.6.04

Incorrect Boot Code Requirement — *Installation and Basic Configuration Guide* (p/n 5990-6028, September 2003): On page 14-3 under the heading “Updating Software in Release 07.6.04 and Later”, the manual incorrectly states that you must update the boot code to version 07.6.04 before updating the software code to 07.6.04. The correct boot code to use is 07.6.02 or later.

Incorrect Statement of Module Availability — *Quick Start Guide* (p/n 5990-6040, September 2003): On page 2-33, in the “Unmanaged Modules” section of table 2-4, the manual incorrectly states that the J4856A Mini-GBIC module has been discontinued. As of October, 2003, HP continues to offer this module.

Summary of Enhancements in 07.6.04

This section summarizes the operating system enhancements in software release 7.6.04. These enhancements are described in the product documentation for software release 07.6.04 or greater, included on the *Documentation CD-ROM* shipped with management modules beginning October 15, 2003. The latest version of this documentation is also available on the HP ProCurve website. (Refer to “Updating Software” on page 6.)

Most features are supported on both Standard and Enhanced Performance (EP) devices. However, some features apply to only one platform or the other. The following tables indicate the platform on which each enhancement is supported.

Note to Users of BGP

Starting with software release 07.6.04, BGP synchronization (**synchronization** command at the BGP level of the CLI) is deprecated and synchronization is always OFF.

In releases prior to 07.6.04, you could enable this command so that the router waits until the Interior Gateway Protocols (IGPs) in the local Autonomous System (AS) have fully exchanged route information before BGP4 advertises the routes to its remote BGP4 neighbors.

Enhancements in 07.6.04

The **EP** and **S** columns in the tables indicate the platforms on which each feature is supported. A “✓” in the **EP** column indicates the feature is supported on Enhanced Performance devices. A “✓” in the **S** column indicates the feature is supported on standard devices.

New Hardware

Software release 07.6.04 provides the following new hardware support.

Enhancement	Description	EP	S
HP ProCurve 9300 2-Port 10-Gigabit Ethernet Module (J8174A)	This release adds support for a new 10-Gigabit Ethernet module with XENPAK optics. This new module uses GBIC-like XENPAK Multisource Agreement (MSA) optics. The XENPAK modules are hot-swappable, and use SC-type connectors	✓	✓

Layer 3 Enhancement in 07.6.04

Enhancement	Description	EP	S
Ability to apply an OSPF distribution list to an interface	Software release 07.6.04 enables you to apply an OSPF distribution list to a physical or virtual routing interface. In releases prior to 07.6.04, you could configure an OSPF distribution list on a global basis only.	✓	✓
Using ACLs to control multicast features	ACLs can now be used to control the following multicast features: • Limit the number of multicast groups that are covered by a static rendezvous point (RP) • Control which multicast groups for which candidate RPs sends advertisement messages to bootstrap routers • Identify which multicast group packets will be forwarded or blocked on an interface	✓	✓
New command to update PIM Sparse forwarding entries	You can update the entries in the static PIM sparse forwarding table by entering the **clear pim rp-map** command. This command can be used after an RP configuration is modified.	✓	✓

Enhancement	Description	EP	S
OSPF Syslog enhancement	You can specify which kinds of OSPF-related Syslog messages are logged.	✓	✓
Change to OSPF show command	Two fields that appeared in the output of the **show ip ospf neighbor** command now appear in the output of a new command, **show ip ospf neighbor detail**.	✓	✓
Concurrent L2/L3 multicast hardware switching	Layer 2 and Layer 3 multicast traffic on tagged and untagged ports can now be forwarded in hardware on EP modules.	✓	
Mirror ports for Policy-Based Routing (PBR) traffic	You can create mirror ports to which Policy-Based Routing (PBR) traffic is copied.	✓	

Layer 2 Enhancement in 07.6.04

Enhancement	Description	EP	S
Ability to configure VSRP-aware security parameters	With the VSRP-aware security enhancement, you can: • Define specific authentication parameters that a VSRP-aware device will use on a VSRP backup switch. The authentication parameters that you define will not age out. • Define a list of ports that have authentic VSRP backup switch connections. The VSRP-aware switch will not use the aware functionality to process VSRP hello packets coming from ports not specified in this list.	✓	✓
MAC address filtering on VEs	You can apply MAC filters to virtual routing interfaces.	✓	✓
VLAN ID matching on EP moduless	The VLAN ID matching feature allows you to bind ACLs to virtual routing interfaces of different VLANs that have tagged ports.	✓	
Enhancement to PVST+ compatibility mode	A port that is in PVST+ compatibility mode due to auto-detection reverts to the default MSTP mode when the port is disabled.	✓	✓
Enhancement to 802.1W	When configuring 802.1W bridge parameters, make sure that the value for **max-age** is greater than the value of **forward-delay**.	✓	✓

Multicast Enhancements in 07.6.04

Enhancement	Description	EP	S
DVMRP support for up to 512 virtual interfaces	In software release 07.6.04, the Distance Vector Multicast Routing Protocol (DVMRP) provides support for up to 512 virtual interfaces.	✓	✓
Ability to configure the PIM Dense prune wait time	The **prune-wait** command enables you to configure the amount of time the router will wait before stopping traffic to a neighboring PIM router.	✓	✓

System-Level Enhancement in 07.6.04

Enhancement	Description	EP	S
		✓	✓
DVMRP support for up to 512 virtual routing interfaces	In software release 07.6.04, the Distance Vector Multicast Routing Protocol (DVMRP) provides support for up to 512 virtual routing interfaces.	✓	✓
Ability to configure the PIM Dense prune wait time	The **prune-wait** command enables you to configure the amount of time the router will wait before stopping traffic to a neighboring PIM router.	✓	✓
Link aggregation enhancements	You can now determine the status of ports that are part of an aggregate link, and determine whether or not Link Aggregation Control Protocol (LACP) messages are being exchanged between the ports.	✓	✓
ACLs to filter ARP	ACLs can now be used to filter ARP request packets.	✓	✓
Enhancements to ToS-based QoS	The T-Flow Module now supports marking of ToS bits.	✓	✓
802.1X port security enhancements	The following enhancements have been made to HP's implementation of 802.1X port security: • Dynamic VLAN assignment • Removal of restrictions on configuring 802.1X port security on route-only ports and virtual routing interfaces • New Syslog messages for 802.1X port security	✓	✓
TSP load sharing on a per-DMA basis	The T-Flow Module supports TSP load sharing on a per-DMA basis. Previous releases supported TSP load sharing on a per-module basis only.		✓
Default sFlow sampling rate	The default sFlow sampling rate now depends on the device being configured.	✓	✓
Terminal length and show terminal commands	The new **terminal length** command allows you to specify the size of a screen during the current CLI session. The **show terminal** command displays the configuration for the terminal length and other commands related to terminal displays.	✓	✓
New ACL configuration requirement for EP	All ACL changes to the running configuration must be followed by a rebind of all ACLs.	✓	
Configurable Layer 4 session log timer	The Layer 4 session log timer interval, which is used for keeping track of packets explicitly denied by an ACL, is configurable.	✓	✓

Enhancement	Description	EP	S
Enhancement to the snSwPortInfoTable	The following are enhancements to the snSwPortInfoTable: • The snSwPortVlanId object has been updated from read-only to read-write access to allow a tagged port to be assigned to a VLAN and to enable dual mode. • The snSwPortTagType has been added to allow the IEEE802.1q tag type embedded in the length/type field of an Ethernet packet.	✓	✓
Displaying the size of the running-config	The output of the **show running-config**, **write terminal**, and **show configuration** commands has been enhanced to display the size of the running-config.	✓	✓
Higher maximum number of Syslog buffer entries supported on Layer 2 Switches	You can configure the Syslog buffer on a Layer 2 Switch to contain up to 1000 entries. Previous releases support up to 100 entries.	✓	✓
New compression algorithm for software images	Beginning with release 07.6.04, a new and improved compression algorithm is used to generate software code images. The new compression algorithm allows the software images to contain more features.	✓	✓
HP Discovery Protocol (FDP) and Cisco Discovery Protocol (CDP)	You can now enable or disable FDP and CDP at the interface level. A new MIB object allows you to enable or disable CDP at the interface level using SNMP.	✓	✓
Path MTU discovery (RFC 1191) support	HP devices support the path MTU discovery method described in RFC 1191.	✓	✓
MTU enhancement for Standard devices	You can configure some Ethernet interfaces on a Standard device to have an MTU of 1518 bytes and others to have an MTU of 1920 bytes.		✓
Flow control enhancement	The HP device generates 802.3x PAUSE frames when the number of buffers available to a module's Buffer Manager (BM) drops below a threshold value.	✓	
Displaying an interface's name in Syslog messages	A new IP configuration option has been added to allow you to display a port or interface name in the Syslog, instead of the port or interface number.	✓	✓
Additions to the **show process cpu** display	The **show process cpu** command now displays CPU utilization statistics for ACL, 802.1.X, NAT, and L2 switching traffic.	✓	✓
ACL comment for ACL with names	You can now add a comment to an ACL that uses a name instead of a number.	✓	✓
Changes to system parameters for PIM and DVMRP	The **system-max dvmrp-max-int-group** and the **system-max pim-max-int-group** commands have been removed since there no longer is a limit to the number of interface groups that can be configured. Three new commands, **system-max multicast-flow**, **system-max dvmrp-mcache**, and **system-max pim-mcache** have been added to define the number of multicast cache entries in the CAM.	✓	✓

Enhancement	Description	EP	S
New compression algorithm for software images	Beginning with boot code release 07.6.02, a new and improved compression algorithm is used to generate software code images. The new compression algorithm allows the software images to contain more features.	✓	✓
HP Discovery Protocol (FDP) and Cisco Discovery Protocol (CDP)	You can now enable or disable FDP and CDP at the interface level. A new MIB object allows you to enable or disable CDP at the interface level using SNMP.	✓	✓
Path MTU discovery (RFC 1191) support	HP devices support the path MTU discovery method described in RFC 1191.	✓	✓
MTU enhancement for Standard devices	You can configure some Ethernet interfaces on a Standard device to have an MTU of 1518 bytes and others to have an MTU of 1920 bytes.		✓
Flow control enhancement	The HP device generates 802.3x PAUSE frames when the number of buffers available to a module's Buffer Manager (BM) drops below a threshold value.	✓	
New **show-portname** command	A new IP configuration option has been added to allow you to display a port or interface name in the Syslog, instead of the port or interface number.	✓	✓
New additions to the **show process cpu** display	The **show process cpu** command now displays CPU utilization statistics for ACL, 802.1.X, NAT, and L2 switching traffic.	✓	✓
ACL comment for ACL with names	You can now add a comment to an ACL that uses a name instead of a number.	✓	✓
New IGMP MIB table	The IGMP Static Group table contains entries for IGMP groups [61315]	✓	✓
Changes to system parameters for PIM and DVMRP	The **system-max dvmrp-max-int-group** and the **system-max pim-max-int-group** commands have been removed since there no longer is a limit to the number of interface groups that can be configured. Three new commands, **system-max multicast-flow**, **system-max dvmrp-mcache**, and **system-max pim-mcache** have been added define the number of multicast cache entries in the CAM.	✓	✓

Details on Applying an OSPF Distribution List to an Interface

An OSPF distribution list filters specific OSPF routes from being installed in the IP route table. To configure an OSPF distribution list, you first configure a standard or extended ACL that identifies the routes to deny or permit, then configure an OSPF distribution list that applies the ACL to incoming route updates.

In releases prior to 07.6.04, the HP device applies the OSPF distribution list to all incoming route updates.

In software release 07.6.04, you can optionally specify on which physical or virtual interfaces to apply an OSPF distribution list. Hence, the HP device can filter incoming route updates on specific interfaces only, instead of globally, on all interfaces.

To apply an OSPF distribution list to an interface, enter commands such as the following:

```
HP9308(config)# router ospf
HP9308(config-pim-router)# distribute-list acl1 in e1/1
```

Syntax: [no] distribute-list < *acl-name* > | < *acl-id* > in [< *interface type* >] [< *interface number* >]

This feature is disabled by default.

The < *acl-name* > parameter specifies the standard or extended ACL name that defines which network(s) to permit or deny.

The < *acl-id* > parameter specifies the standard or extended ACL number that defines which network(s) to permit or deny.

The **in** command applies the ACL to incoming route updates.

The < *interface type* > parameter identifies the interface type (i.e., **e** (ethernet) or **ve** (virtual)) on which to apply the ACL.

The < *interface* > parameter specifies the interface number on which to apply the ACL. Enter only one valid interface number. If necessary, use the **show interface brief** command to display a list of valid interfaces. If you do not specify an interface, the HP device applies the ACL to all incoming route updates.

Details on Configuring VSRP-Aware Security

Virtual Switch Redundancy Protocol (VSRP) is a proprietary protocol that provides redundancy and sub-second failover in Layer 2 and Layer 3 mesh topologies. If an active Layer 2 or Layer 3 VSRP switch becomes unavailable, a VSRP backup takes over as the active device and continues forwarding traffic for the network.

A VSRP-aware device is an HP device that is not itself configured for VSRP, but is connected to an HP device that is configured for VSRP. A VSRP-aware device can failover its link to a new VSRP master in sub-second time, by changing the MAC address associated with the redundant path.

NOTE: An HP device must be running software release 07.6.01b or later to be a VSRP device or VSRP-aware device.

A VSRP-aware device determines which VSRP device is master by listening to incoming VSRP hello packets from the VSRP backup switch. However, it is possible for a VSRP-aware device to receive VSRP hello packets that are not generated by an authentic VSRP backup switch.

Software release 07.6.04 enhances the security of VSRP-aware switches against unauthorized VSRP hello packets by enabling you to configure VSRP-aware security parameters.

Without VSRP-aware security configured, a VSRP-aware device passively learns the authentication method conveyed by the received VSRP hello packet. The VSRP-aware device then stores the authentication method until it ages out with the aware entry.

With VSRP-aware security, you can:

- Define the specific authentication parameters that a VSRP-aware device will use on a VSRP backup switch. The authentication parameters that you define will not age out.
- Define a list of ports that have authentic VSRP backup switch connections. For ports included in the list, the VSRP-aware switch will process VSRP hello packets using the VSRP-aware security configuration. Conversely, for ports not included in the list, the VSRP-aware switch will not use the VSRP-aware security configuration.

If VSRP hello packets do not meet the acceptance criteria, the VSRP-aware device forwards the packets normally, without any VSRP-aware security processing.

Specifying an Authentication String for VSRP Hello Packets

The following configuration defines **pri-key** as the authentication string for accepting incoming VSRP hello packets. In this example, the VSRP-aware device will accept all incoming packets that have this authorization string.

```
HP9300(config)# vlan 10
HP9300(config-vlan-10)# vsrp-aware vrid 3 simple-text-auth pri-key
```

1vsrp-aware vrid < *vrid number* > simple text auth < *string* >

Specifying no Authentication for VSRP Hello Packets

The following configuration specifies no authentication as the preferred VSRP-aware security method. In this case, the VSRP device will not accept incoming packets that have authentication strings.

```
HP9300(config)# vlan 10
HP9300(config-vlan-10)# vsrp-aware vrid 2 no-auth
```

Syntax: vsrp-aware vrid < *vrid number* > no-auth

The following configuration specifies no authentication for VSRP hello packets received on ports 1/1, 1/2, 1/3, and 1/4 in VRID 4. For these ports, the VSRP device will not accept incoming packets that have authentication strings.

```
HP9300(config)# vlan 10
HP9300(config-vlan-10)# vsrp-aware vrid 4 no-auth port-list ethe 1/1 to 1/4
```

Syntax: vsrp-aware vrid < *vrid number* > no-auth port-list < *port range* >

< *vrid number* > is a valid VRID (from 1 to 255).

no-auth specifies no authentication as the preferred VSRP-aware security method. The VSRP device will not accept incoming packets that have authentication strings.

simple-text-auth < *string* > specifies the authentication string for accepting VSRP hello packets, where < *string* > can be up to 8 characters.

port-list < *port range* > specifies the range of ports to include in the configuration.

Multicast Enhancement in 07.6.04

DVMRP Enhancement

Software release 07.6.04 provides support for up to 512 virtual interfaces with the Distance Vector Multicast Routing Protocol (DVMRP). Earlier software releases provide support for up to 256 virtual interfaces.

Configuring the Prune Wait Time

PIM Dense is a flood-and-prune protocol. It floods traffic to multicast routers every three minutes (the default value) or as indicated by the **prune-timer** command (from 10 seconds to 60 minutes). It then prunes (removes) multicast neighbor routers that do not want the traffic, as determined by prune messages sent from these multicast neighbor routers to the upstream PIM router. The upstream PIM router waits three seconds before stopping traffic to multicast neighbor routers that send prune messages. During these three seconds, other neighbors on the same interface that want the traffic can send join messages to override the prune messages.

A new CLI command, **prune-wait**, allows you to configure the amount of time a PIM router will wait before stopping traffic to neighbor routers that do not want the traffic. The value can be from zero to three seconds. The default is three seconds. A smaller prune wait value reduces flooding of unwanted traffic.

A prune wait value of zero causes the PIM router to stop traffic immediately upon receiving a prune message. If all multicast neighbor routers are on separate virtual interfaces in a Layer 3 environment, you can safely configure the prune wait time to zero because traffic to neighbors is independent.

To set the prune wait time to zero, enter the following commands:

```
HP9308(config)# router pim
HP9308(config-pim-router)# prune-wait 0
```

Syntax: prune-wait < *time* >

where < *time* > can be 0 - 3 seconds. A value of 0 causes the PIM router to stop traffic immediately upon receiving a prune message. The default is 3 seconds.

Viewing the Prune Wait Time

To view the prune wait time, enter the following command at any level of the CLI:

```
Routing Switch(config)#show ip pim dense


Global PIM Dense Mode Settings
```

```
Hello interval: 60, Neighbor timeout: 180
Graft Retransmit interval: 180, Inactivity interval: 180
Route Expire interval: 200, Route Discard interval: 340
Prune age: 180, Prune wait: 3
```

Where To Get More Information

Table 8. Switch and Router Feature Documentation

Title	Contents

Installation and Basic Configuration Guide	• Installation
	• Basic Features
	  • System (SNMP, SNTP, Syslog, broadcast and multicast throttling)
	  • Port configuration (speed, mode)
	  • Layer 2 (MAC table parameters, MAC filters, broadcast and multicast filters, port locks)
	  • Parameter table resizing
	  • Port monitoring
	• Link Aggregation
	• Spanning Tree Protocol
	• Virtual LANs
	• Layer 2 Multicast
	• Base Layer 3
	• Updating Software
	• Hardware Specifications
	• RFCs

Security Guide	• Security (passwords, user accounts, AAA, RADIUS, and TACACS/TACACS+) • Secure Shell (SSH) • Denial of Service Protection

Table 8. Switch and Router Feature Documentation (Continued)

Title	Contents
Advanced Configuration and Management Guide	• QoS • ACLs • EP rate limiting • Standard rate limiting • IP • RIP • IP Multicast • OSPF • BGP4 • Network Address Translation • VRRP and VRRPE • IPX • AppleTalk
Router Command Line Interface Reference	Syntax information for all CLI commands. See the "Command List" chapter for a complete list of the CLI commands and page references to syntax information.

Software Fixes

- **AAA —** When TACACS+ is the primary authentication method for securing Telnet/SSH access (aaa authentication login default tacacs+ local command), and the TACACS server is not available, AAA authorization and authentication via local user accounts are slow.
- **ACL —** An inbound ACL on an outside NAT interface causes the HP device to deny IP fragments with non-zero offset values instead of permitting them.
- **ACL —** If you copy a configuration file from the TFTP server to the running configuration, and the file has ACLs and ACL remarks, the HP device changes the order of the ACL remarks.
- **ACL** – You can configure a standard ACL to permit Telnet access and log any Telnet access to the Syslog. However, in previous releases, permit traffic for Telnet access were not being entered in the Syslog.
- **ACL** – NAT for UDP traffic was being disabled when ACLs were applied to outside interfaces. This problem occurred when you bound an ACL on an outside NAT interface and the traffic was initiated from outide the network.
- **ACL, NAT —** When you bind an inbound ACL to an outside NAT interface, NAT translation does not occur on the EP module.
- **Appletalk —** Appletalk packets leak over STP blocked ports, causing next-hop routes to change. This problem occurs after the STP status of a link on a router changes from forwarding to blocking.
- **AppleTalk —** The Routing Switch does not send a NetInfoReply packet if it does not have an AppleTalk ARP (AARP) entry. This occurs when the port receiving a GetNetInfo packet is a tagged port and the AARP for a requester client does not exist on the Routing Switch.
- **ARP** – When the modules were hot-swapped, they experienced a failover. After the device returned to normal operation, its virtual routing interfaces were unreachable for a long period of time. This occurred because ARP request packets that were being sent to the downstream routers never reached the routers. The packets were to inform the downstream routers of the new MAC addresses of the virtual routing interfaces after the

hot-swap occurred.

- **Autonegotiation** (EP only) – On EP modules, ports were going into BLOCKING mode when the speed of the remote port that was connected to a host was changed from full-duplex to half-duplex while the port was in autonegotiation mode. Although this may seemed to be related to spanning tree, it was due to the change in the port speed while the port was in autonegotiation mode. The port was not being initialized after the change and packets were being looped back to the port.
- **BGP —** An invalid address in BGP route flap dampening causes a software reload.
- **BGP —** After issuing the clear ip bgp neighbor all command, all aggregate routes previously configured using the aggregate-address command do not function properly. The HP device does not aggregate BGP routes for those configured aggregate routes.
- **BGP4+ —** The Routing Switch displays a negative MED (metric default) when the value configured is greater than 2147483647.
- **CLI —** In global CONFIG mode, after entering the command module < *slot-num* > ?, the HP device displays a partial (incomplete) list of installed modules. Also, you cannot configure a module that is not on the list.
- **CLI —** The show fdp neighbor < *portnum* > command output does not display all FDP and CDP neighbors.
- **CLI —** The show fdp neighbor detail command output displays an incorrect VLAN ID number.
- **CLI —** Parsing fails for CLI commands which contain yes / no parameters. The parsing of an initial "no" in the command line (removing a configuration command) always works. The parsing error occurs only when the command is enabled.
- **CLI —** The Routing Switch reports a false power supply failure.
- **CLI** – The CLI (using console, Telnet, or SSH) froze when the number of OSPF border routers to be displayed is greater than the number that can fit on one page. Pressing CTRL + C recovers the CLI.
- **DVMRP** – Entering the **show ip dvmrp** or **show ip pim** command for an interface displayed the error message `"Error - 0 not between 1 and 256".` Furthermore, multiple “router pim” sections appeared in the display.
- **General** – Software reboots occurred if an IP policy environment has one or more virtual routing interface defined. This occured even if there is no IP policy defined on the virtual routing interface. The problem can happen on both Chassis devices.
- **IP Stack** – HP devices were learning all destination IP addresses with a MAC address of ff-ff-ff-ff-ff-ff. Beginning with software release 07.5.06 and 07.6.04, broadcast Ethernet addresses will not be accepted as a valid source MAC address in the ARP table to prevent this problem from occurring.
- **IGMP** – When a router received an mtrace request from its directly attached host and the request is for a directly attached multicast server, the router did not send a response to the host. Instead, the response was sent to the multicast server.
- **IGMP —** The show ip igmp group command output does not contain enough spaces between displayed values. This causes IP group addresses and other values to display incorrectly. For example, an IP group address of 239.255.255.255 appears as 239.255.255.25.
- **IP Policy —** If you add a new port to a VLAN that has PBR configured, the HP device does not apply PBR to the new port.
- **IP Stack —** When ip route < *ip-addr* > < *ip-mask* > null0 commands are in the configuration, hot swapping the blades can cause a software reload.
- **IP Stack —** OSPF convergence causes multiple default gateway address entries in the route table. If the gateway addresses do not match, the HP device cannot properly route packets to these destinations.
- **IP Stack —** A software reload occurs when the HP device forwards packets to a null interface via a static route.
- **IP Stack —** Packet corruption causes a software reload.
- **EP Rate Limiting —** High CPU rate (99% usage) occurs in configurations with rate limiting and ACLs using

rule-based CAM.

- **Login/Logout —** Special control characters from TACACS+ disable authentication.
- **Mirroring —** With port mirroring configured, the HP device sometimes performs a software reload.
- **MSDP —** When you configure an MSDP peer using a loopback interface, the Routing Switch is unable to create a TCP session. Note that this does not occur when you configure an MSDP peer using a physical interface.
- **NAT —** In configurations with inside-to-outside NAT and PBR, the HP device drops out-of-sequence IP fragmented packets.
- **NAT —** Outside NAT does not work if applied to a virtual routing interface. To use the feature, apply it directly to a physical port.
- **NAT** – In previous releases, when a client from outside the network pinged a server that is inside the network, the HP switch to which the server is connected responded to the ping, if ICMP packets are sent. In this release, HP switch will allow the server inside the network to reply to ping requests from clients outside the network if the following requirements are met:
  - The packets sent are ICMP packets.
  - A source static NAT has been defined for the server in the HP switch.
- **NAT** – On the T-Flow, NAT and sflow did not work properly with UDP streaming media. In this release, UDP streaming media is disabled by default. (TCP streaming media works as it did before.) To enable UDP streaming, you must explicitly enable it. To do this, use the **ip nat enable stream-media** command.
- **NetFlow —** Enabling ip route-cache flow on an interface causes a significant decrease in traffic throughput on the port.
- **OSPF** – OSPF may fail to learn a new route after receiving link state advertisement with Appendix E LSA ID format. In a reported case, a new static route was created and the old one was deleted. OSPF did not have the new route in its routing table.
- **OSPF —** Two equal-cost routes remain in the IP route table even if the OSPF cost changes on one link. This happens when two routes (same network) redistribute into OSPF with the same metric type 1.
- **OSPF —** The HP device does not dynamically apply the default metric to external routes imported into OSPF.
- **Other —** The HP device allows configuration of the same same password for super user and Telnet access. This can cause the super user session to lock up.
- **Other —** IPC packet corruption causes a software reload.
- **Other —** The Routing Switch reports CPU forwarding packet loss.
- **PIM** (Standard modules only) – When a router forwards multicast traffic downstream, it did not change the packet's source MAC address to its own. This problem occurred when using PIM-SM and PIM-DM during the first three minutes of the process.
- **PIM Dense —** The HP device copies hardware-switched packets to the CPU for one minute every four minutes. This occurs only on EP modules and tagged ports.
- **PIM SM** – In software release 07.6.01, a port that had a rule-based ACL dropped multicast traffic.
- **PIM Sparse —** Protocol Independent Multicasting Sparse Mode (PIM SM) traffic snooping (ip pim-snooping command) does not work correctly. The show ip multicast command output classifies a port that receives a PIM hello message as a forwarding port, even though the port does not take participate in multicasting.
- **PIM Sparse —** With multicast enabled, the HP device performs a software reload. This problem occurs when many multicast sessions, such as source or group sessions, share the same group.
- **Port Mirroring** – When you configured a port to mirror the traffic on another port, that port displayed twice the number of broadcast packets than the port that it was mirroring. For example, if you configured Port 2/10 to mirror Port 2/5, Port 2/10 showed 200 broadcast packets, while Port 2/5 showed only 100. Both ports should have showed 100.

- **Port Security —** A securely configured MAC address causes a security port violation.
- **Rate Limiting** (EP modules only) – In some cases, outbound rate limiting took a long time (over 10 minutes) to take effect.
- **RSTP —** A new VLAN added to a VLAN group does not inherit the RSTP configuration of the master VLAN in a topology group.
- **RSTP - 802.1w —** When a HP device dynamically creates or deletes a trunk, and the HP device is a root bridge, the root port on a connected device flaps.
- **sFlow —** If you change the sampling rate on an individual port on an Ethernet module in a device managed by T-Flow, sampling for all ports on the module may not occur at the expected rates.
- **sFlow —** Enabling sFlow causes high CPU usage under heavy traffic conditions.
- **sFlow** – If sFlow is enabled with more than one sFlow collector configured, the system may crash due to out of UDP buffers, when the traffic has any actual sFlow packet whose size is close to the largest supported packet size.
- **Static MAC entries** (Standard modules only) – Packets were dropped if you configured static MAC entries with multiple physical ports and the outgoing ports were on a different slot. A **show cam** command would also show the incorrect forwarding ID for the interface.
- **SNMP** – A Get/Get Next request for the object snChasFanOperStatus returned a different response from a Get Bulk request. For example, if a Get/GetNext request was used for snChasFanOperStatus on a FastIron 4802, the reply was normal(1). However, if a GetBulk request was used, the reply was failure(3) even though the fans were operating normally.
- **SNMP Management —** Incorrect DMA initialization causes a software reload.
- **SNMP Management —** The Routing Switch doesn't generate a VSRP SNMP trap when a VSRP topology change occurs.
- **SNMP Management —** The Routing Switch doesn't generate an SNMP trap when a Metro Ring Protocol (MRP) failover occurs.
- **SNMP Management —** The counter for unknown protocols increases when the HP device receives OSPF hello packets. This indicates that the HP device is treating multicast traffic as an unknown protocol.
- **Spanning Tree —** Disabling and enabling an untagged, free port in a member VLAN of a topology or STP group causes the port to block all traffic.
- **Static Routes —** When the HP device redistributes equal cost static routes into BGP, and a static route goes down, the next hop is not updated.
- **System —** When a port operates at 100-half duplex, the HP device generates runt frames, CRCs, and alignment errors, eventually causing the port to lock up. Port counters show the ports as transmitting packets, but not receiving packets.
- **System —** CPU and memory issues cause a software reload.
- **Topology Groups —** Adding a non-configured master VLAN and member VLAN to a topology group causes a software reload.
- **Trunking —** In configurations where a 4-port tagged trunk group belongs to over 300 VLANs, if the entire trunk group is disabled physically, the HP device can take up to 15 seconds to bring down the trunk links over all the VLANs.
- **Trunking** – Enhancements that allowed Layer 3 hardware forwarding functions to use the server trunk FID for server trunk port caused an HP device to drop packets when the trunk server is configured in a one-armed-routing situation. The fix in this release does not to use the server trunk FID if the port is configured with one-armed-routing port.
- **Trunking** – A device contained an active and standby management modules. These modules were configured with virtual routing interfaces that were assigned to a VLAN. The VLAN contained a cross-module trunk with ports on both the active and the standby management modules.

- **VLANs** (15-slot chassis only) – In release prior to 07.6.02, you could configure only up to 2195 Layer 2 VLANs on a 15-slot Chassis device. The **system-max vlan** < *num* > command allowed you to allocate a higher number of VLANs, but the software allowed you to actually create only 2195 of the allocated VLANs. In release 07.6.02, this restriction was removed. You can create the full number of allocated Layer 2 VLANs on a 15-slot Chassis device, up to 4095.
- **VSRP —** If you add a switch to the core network, and the switch you are adding has VSRP enabled, the HP device changes the VSRP Last Port state.
- **Web Management —** After a software reload, the running configuration file does not display the no web-management hp-top-tools configuration, even though TCP port 280 is disabled.
- **Web Management —** The front panel display of double-wide chassis modules (modules that occupy two chassis slots) is not aligned correctly on some browsers. This issue affects the picture.htm page and occurs with the following browsers:
  - Netscape Communicator 4.78 Linux 7.2
  - Mozilla 0.9.2.1 for Linux 7.2
  - Mozilla 1.0.1 for Windows
  - Mozilla 1.1 for Windows
  - Mozilla 1.2 Alpha for Windows
  - The picture.htm page displays correctly for double-wide modules in the following browsers:
  - Netscape Communicator 4.78 Windows
  - Internet Explorer 6.0.2600.000IC
- **Web management interface** – When a tagged port is added to an existing VLAN using the Web management interface, the tagged port did not forward traffic to the device to which it was connected.

Known Issues

Single STP Issues When Migrating from 06.6.*x* to 07.5.*x* or Greater

Overview

Software releases 07.x support up to 4095 port-based VLANs in a single spanning tree. This support required a change to the position of the port-based VLAN commands in the running-config and startup-config file.

- In software release 06.6.*x*, the VLAN commands are placed before the **spanning-tree single** command.
- In the 07.*x* software releases, the **spanning-tree single** command is placed before the VLAN configuration commands.

As a result of the changed command positions, if you boot a device using software release 07.5.x but also load a startup-config file created using software release 06.6.x, the CLI parser does not find the **spanning-tree single** command before the VLAN commands. The parser therefore assumes that the single STP feature is not enabled. When the device finishes booting, the device contains a separate spanning tree for each VLAN on which STP is enabled, instead of a single spanning tree consisting of all the VLANs on which STP is enabled.

Migration Procedure

NOTE: You need to use this procedure only if you are updating a device running software release 06.6.x (and using single STP) to the 07.x software releases.

To migrate your single STP configuration from 06.6.*x* to 07.5.*x*:

- Make a backup copy of the startup-config file. You will need this file if you decide to revert to the 06.6.*x* release for any reason.
- Boot the device using software release 07.5.*x*.

- Disable single STP.
- Enable STP (not single STP) in each of the port-based VLANs that you want to include in the single spanning tree.
- Enable single STP.
- Save the configuration. You cannot use the configuration you saved using 06.6.*x* on a device running 07.*x*.

Saving a Backup Copy of the Service's Startup-Config File

1. Make sure the device has IP access to a TFTP server.
2. Enter one of the following commands at the Privileged EXEC level of the CLI to copy the device's startup-config file onto the TFTP server:
   - **copy startup-config tftp** < *ip-addr* > < *filename* >
   - **ncopy startup-config tftp** < *ip-addr* > < *from-name* >

Completing the Migration

1. Boot the device using software release 07.5.*x*.
2. Enter the following command at the global CONFIG level of the CLI to disable single STP:
   - **no spanning-tree single**
3. Enable STP within the port-based VLANs that will be members of the single spanning tree. When you re-enable single STP, all the VLANs in which you enabled STP will become members of the single spanning tree. Other VLANs (in which STP is disabled), will not become part of the single spanning tree.

   To enable STP in a VLAN, enter the following command at the global CONFIG level of the CLI to exchange the CLI to the configuration level for that VLAN:
   - **vlan** < *vlan-id* >

   To enable STP within the VLAN, enter the following command:
   - **spanning-tree**
4. Enable single STP. To do so, enter the **exit** command to return to the global CONFIG level of the CLI, then enter the following command to enable single STP:
   - **spanning-tree single**
5. Save the configuration changes to the startup-config file.
6. Reload the 075.*x* software.

NOTE: When you reload, use the startup-config file you saved in Step 5. If you try to use a startup-config file saved while running 06.6.*x*, the single STP configuration will not be loaded.

Known Software Issues.

Table 9. Known Software Issues in Release 07.6.04

Category	Description
Gigabit Copper Forwarding Modules	The J4895A 16-port gigabit forwarding module supports 100 Mbps or 1000 Mbps operation in full-duplex mode only. Half-duplex mode is not supported.
IP Stack	**Symptom:** Although rare, in some configurations, the Management Processor (MP) and T-Flow Switching Processor (TSP) routing tables may not synchronize, causing routing problems on the network. **Workaround:** To determine if the MP and TSP routing tables are out of sync, log in to the TSP and enter the command **sh ip route stat**. If the routing tables are not in sync, enter the command **vm bp-route-recover** at the global configuration level of the CLI. This command causes the routing table to automatically redownload whenever the MP and TSP routing tables don't match. To disable automatic routing table downloads, enter the command **no vm bp-route-recover**. This workaround has the following limitations: • The **recover** command works only on TSP1, and not on other TSP CPUs. • The automatic routing table download is limited to once every 5 minutes.
Jumbo IP Packets	**Symptom:** The 2-port 10-Gigabit Ethernet Module does not forward Layer 2 and Layer 3 jumbo packets if only one port is jumbo-enabled. **Workaround:** Enable jumbo packets on both ports of the 2-port 10-Gigabit Ethernet module.
NAT	**Symptom:** HP does not support streaming protocols, such as RTSP/MMS, if IP NAT inside destination static is configured. **Workaround:** None at this time
NetFlow	**Symptom:** With auto-negotiation enabled, if you disconnect the TX cable on a 10-Gigabit Ethernet port (port 49 or 50), the **show interface** command output indicates that the link is down. However, the active LED indicates that the link is up. This occurs because the Rx signal determines the status of the LED. **Workaround:** None at this time. This is a known hardware limitation.
Other	**Symptom:** When two EP ports are connected via fiber, the following occurs: • Disconnecting the TX cable on a local port causes the local port status to stay "up", but the remote port status is "down". • Disconnecting the RX cable on a local port causes the local port status to go "down", but the remote port status is "up". **Workaround:** Enable the UDLD feature. See the Installation and Basic Configuration Guide.
PIM Sparse	**Symptom:** If you downgrade from software release 07.6.04 to 07.6.01 or earlier, the Routing Switch removes the PIM Sparse Rendezvous Point (RP) address from the running configuration. This is a forward compatibility issue. Starting with software release 07.6.04, you can limit the number of multicast groups covered by a static RP using standard ACLs. The CLI command for this feature is **rp-address < *ip-address* > [< *access-list-num* >]**. Software releases 07.6.01b and earlier do not allow you to use ACLs with static RP configurations. In 07.6.01b and earlier, the CLI command for creating an RP address is **rp-address < *ip-address* >**. Thus, if you downgrade from 07.6.04, the software does not recognize the extra parameter and the Routing Switch rejects the command.
QOS	For IP ToS-based QoS, all virtual routing interfaces on a given IPC must have the same trust level and marking settings.

Table 9. Known Software Issues in Release 07.6.04

Category	Description
Rate Limiting	All ports on the 16-port EP Gigabit Ethernet module accept the rate limiting policy constraints of a 1 Gigabit Ethernet port, even when the port speed is configured at 100 mbps.
Rate Limiting	**Symptom:** If you configure Adaptive Rate Limiting and ACLs on the same port, rate limiting stops working on the port and only the ACLs take effect. **Workaround:** None at this time
sFlow	**Symptom:** The sFlow sampling rate does not take effect when you change from the default sampling rate. **Workaround:** Reboot the device
sFlow	sFlow and port monitoring are not supported together. If you enable one of these features on any port on the device, the other feature cannot be enabled. To use sFlow, make sure port monitoring is not enabled on any of the device's ports.
sFlow	A global sampling rate of 1 is not supported on an EP management module. If you set the global sampling rate to 1, sFlow does not sample any flows.
Spanning Tree	**Symptom:** In a six-node topology with more than 1000 VLANs and 802.1w (Rapid Spanning Tree Protocol (RSTP) enabled, if one trunk fails, traffic convergence takes up to 15 seconds. This occurs in configurations with trunks and more than 1000 VLANs. In this case, if a trunk fails, the HP device sends a BPDU to the root bridge and its connected non-roots after six seconds, as determined by the hello-time interval. The six-second delay causes a timeout in the non-root bridges, which have a shorter timeout value for 802.1w ports. **Workaround:** Set the hello-time value to 4 (**span hello-time 4**), so that the timeout period is 12 seconds instead of 6 seconds.

SSH	**Symptom:** SSH does not automatically failover to the standby module. If you configure an SSH key on a redundant management module, and the primary management module fails, the standby module will not have the RSA key.
	Workaround: To work around this issue, you must configure the host RSA public and private key pair for SSH on the standby module. Enter the following commands:
	`HP9308(config)# crypto key generate rsa`
	`HP9308(config)# wri mem`

Trunking	**Symptom:** For Layer 3 server trunks configured on EP devices, load sharing does not work properly when incoming traffic ports are managed by the same IPC as the server trunk ports. This issue applies only to routing switch images. **Workaround:** None at this time
Trunking	Eight-port trunk groups are not supported on the EP 48-port 10/100 forwarding modules (J4881A and J4889A). This issue does not affect four-port trunk groups.
VLANs	Hardware flooding for Layer 2 multicast and broadcast packets (configured with the **multicast-flooding** command) cannot be used in conjunction with spanning tree on the same VLAN. This could cause multicast packets to be forwarded on blocked ports.

HP ProCurve Routing Switch 9300M Series Modules

Table 10 lists both currently available and discontinued modules.

Table 10. Module Options

Module Type	Part Number and Description	Module String
T-Flow Modules (T-Flow)	**J4879A** HP ProCurve 9300 T-Flow Module version 1 (0-port)	0-port-tf1-management-module
EP Redundant Management Modules	**J4885A** HP ProCurve 9300 EP 8-Port Mini-GBIC Redundant Management Module	EP-8-port-mini-GBIC-management
EP Non-Management Modules	**J4881A** HP ProCurve 9300 EP 48-Port 10/100-TX RJ-45 Module	EP-48-port-10/100-TX-RJ45-module
	J4889A HP ProCurve 9300 EP 48-Port 10/100-TX Telco (RJ-21) Module	EP-48-port-10/100-TX-telco-module
	J4894A HP ProCurve 9300 EP 16-Port Mini-GBIC Module	EP-16-port-mini-GBIC-module
	J4895A HP ProCurve 9300 EP 16-Port 100/1000-T Module	EP-16-port-100/1000-T-module
Redundant Management modules (M2 and M4)	**J4845A** HP ProCurve 9300 GigLX Redundant Management Module (8-port)	8-port-gig-management-module *Discontinued*
	J4846A HP ProCurve 9300 GigSX Redundant Management Module (8-port)	8-port-gig-management-module *Discontinued*
	J4847A HP ProCurve 9300 Redundant Management Module (0-port)	0-port-management-module *Discontinued*
	J4857A HP ProCurve 9300 Mini-GBIC Redundant Management Module (8-port)	8-port-gig-m4-management-module *Discontinued*
Management modules (M1) (HP 9304M and HP 9308M only. These modules will not work on the 9315M)	**J4141A** HP ProCurve 9300 10/100 Management Module (16-port)	16-port-copper-management-module *Discontinued*
	J4144A HP ProCurve 9300 Gigabit SX Management Module (8-port)	8-port-gig-management-module *Discontinued*
	J4146A HP ProCurve 9300 Gigabit 4LX/4SX Management Module (8-port)	8-port-gig-management-module *Discontinued*

Module Type	Part Number and Description	Module String
Unmanaged Modules	**J4140A** HP ProCurve 9300 10/100 Module (24-port)	24-port-copper-module
	J4142A HP ProCurve 9300 100Base FX Module (24-port MT-RJ)	24-port-100fx-module *Discontinued*
	J4143A HP ProCurve 9300 Gigabit SX Module (8-port)	8-port-gig-module *Discontinued*
	J4145A HP ProCurve 9300 Gigabit 4LX/4SX Module (8-port)	8-port-gig-module *Discontinued*
	J4842A ProCurve 9300 1000Base-T Module (8-port)	8-port-gig-copper-module *Discontinued*
	J4844A HP ProCurve 9300 GigLX Module (8-port)	8-port-gig-module *Discontinued*
	J4856A HP ProCurve 9300 Mini-GBIC Module (8-port)	8-port-gig-module *Discontinued*
	J4891A HP ProCurve 9300 1-port 10-Gb Module	1-port-10Gig-module *Discontinued*
	J8174A HP ProCurve 9300 2-port 10-Gb Module	2-port-10Gig-module
	J8178A HP ProCurve 9300 EP 24-Port 100Base-FX Module	EP 24 Port 100Base-FX Module

Edition 2, March 2004
Manual Part Number
5990-6027